The Cyber Threat to the Public Sector: Considerations for Federal, State and Local Governments

By: Mike Kelly, Head of Cybersecurity and Technology Controls, Commercial Banking
The volume and variety of cyber threats today cross all sectors and industries. Increasingly, federal, state and local governments are targets as hackers, organized criminals, foreign countries and others attempt to steal or manipulate sensitive data.

Cyberattacks often target government networks to gain access to sensitive personal information of citizens and employees, as well as proprietary software, strategic plans and other information. The challenge for any agency is to identify threats and vulnerabilities, invest in risk mitigation and continually assess and improve cybersecurity efforts.

Learn the scope of this challenge, the kinds of threats already occurring and steps every level of government can take to help prevent future cyberattacks.
Attacks Against Governments on the Rise

Cyberattacks against local, state and federal government agencies are increasing. A 2016 Government Accountability Office report found that between 2006 and 2015, the federal government alone saw a 1,300 percent increase in information security incidents.

Different types of perpetrators can initiate cyber threats, and their motivations vary widely. Foreign nations may seek to obtain sensitive voter information; criminals may steal government employee data to sell and commit fraud; and hacktivists—those motivated by ideology rather than profit—advance their agenda through targeted attacks. What is more, methods of attack vary, including ransomware that encrypts data, email-based social engineering attacks (which trick the recipient into opening a malicious link or attachment) and zero-day exploits (i.e., when a hacker exploits a previously unknown security vulnerability before it’s been patched).

**CYBERATTACKS STRIKE EVERY LEVEL OF GOVERNMENT**

Some of the most serious attacks against public sector networks in recent years include:

**Federal government:** Hackers have breached data files and websites of federal offices and agencies to gain the sensitive personal information—including Social Security numbers and home addresses—of millions of employees, contractors and taxpayers.

**State government:** Hackers compromised various government websites across four states, littering the sites with pro-terrorist propaganda, though it’s unclear whether a terrorist group was behind the hacks.

**City government:** As part of local protests, hacktivists attacked a city government’s website, bringing it offline for at least 16 hours. This was an example of a rising trend in hacktivist activity targeting state and local governments.
Government Levels Face Different Challenges, Needs

Despite the fact that cybersecurity is a priority for public sector chief information officers and chief information security officers, government agencies at all levels continue to experience difficulties. At the federal level, successful cyberattacks are often the result of negligent insider actions (e.g., opening a malicious email attachment), followed by zero-day attacks and third-party (e.g., vendor) error, according to a survey of local, state and federal security practitioners performed by Ponemon Institute and sponsored by HP.

At the local and state level, however, a basic failure to fix known vulnerabilities is the leading reported cause to blame. Local and state governments often are challenged by a lack of budgetary and skilled personnel resources to manage cyber risks effectively. The Ponemon survey found that only 28 percent of local and state respondents cited a “very high” ability to recover from a cyberattack, and just 19 percent reported a “very high” ability to prevent an attack.

“ONLY 28 PERCENT OF LOCAL AND STATE RESPONDENTS CITED A 'VERY HIGH' ABILITY TO RECOVER FROM A CYBERATTACK”
EXAMPLES OF GOVERNMENT VULNERABILITIES AND SOLUTIONS

Publicly available contracts
To provide transparency to the public and comply with Freedom of Information Act requirements, government entities often post contracts on their websites. Criminals have used contract information to impersonate an employee of the contractor and request new payment instructions for the contract from the government entity’s accounts payable or vendor management teams.

Solution: Implement procedures to document who is able to change vendor payment instructions and validate all changes with vendors by calling them at a known telephone number or initiating small test payment transactions.

Employee information
Information for public sector officials (such as names, email addresses and phone numbers) is available to the public. Criminals can use a spoofed email address or phone number to try to execute an emergency transaction, or they may try to dupe an employee into processing a transaction at the urging of someone they believe is a public official or a superior.

Solution: Train employees to investigate any requests and validate transactions with appropriate hierarchy.

Malware
Cyber attackers can infect government computers with malware, which can then be used to execute large transactions from outside the country and direct funds to accounts controlled by criminals.

Solution: Educate employees not to open suspicious emails or click on unknown links. Use security features to reduce the ability to execute freeform wires, and make sure you have appropriate input to approve wires and wire templates.
Moving Toward Cybersecurity Maturity

In May 2017, President Trump signed an executive order to improve the cybersecurity of federal networks and critical infrastructure. The order calls for a risk management approach to address cyber threats. This is in line with industry standards and best practices to reduce risk, given that there is no single tactic or tool that can guarantee data confidentiality, integrity and availability.

Rather than focusing all resources on keeping bad actors out of a network, organizations should adopt a layered, risk-based suite of tools, policies, training and ongoing assessments to make systems more secure and attempts to obtain data easier to spot. Even as threats change, there are four hallmark components of any effective cyber risk management effort.

1. MAKE CYBERSECURITY A PRIORITY

Managing cyber risk should stem from the highest levels of a government entity. The consequences of a breach are so great—including issues related to national security and election integrity—and the resource demands so substantial that cybersecurity should be viewed as a strategic priority for the entire organization.

Leaders should bring together the appropriate resources and stakeholders to implement a holistic cyber risk management program. The cyber risk justifies that level of governance and should be viewed in the same way institutional risk is viewed.

2. SECURE THE WEAKEST LINK

The weakest link in a cybersecurity chain is often the employee using a network computer or mobile device connected to the organizational network. For instance, an employee could make the mistake of opening a harmful email that appears to come from a government contractor.

To educate employees, government entities should hold cyber breach exercises at least biannually. Training and awareness programs must describe the types of threats that employees may face, the actions they should take and to whom the threat should be reported. The more employees are tested and the more robust their training, the more diligent they will be.

Indeed, a SANS Institute study found that without cybersecurity training, 30 to 60 percent of individuals fell for a social engineering attack (e.g., an email with a malicious attachment). After six to 12 months of quarterly training, those rates dropped to 19 percent; with monthly training, susceptibility rates fell to 5 percent.
3. STRIVE FOR CYBERSECURITY CAPABILITY MATURITY

A leading concept in cybersecurity is “maturity,” which refers to how fully an organization’s cyber risk management efforts align with and address threats, priorities and organizational objectives.

One essential resource in this regard is the National Institute of Standards and Technology Cybersecurity Framework (CSF). The CSF, and its affiliated self-assessment toolkit, helps organizations set benchmarks, identify priorities, implement risk management tactics, measure improvement and adopt appropriate changes. Using this approach, government entities can drive cybersecurity capability maturity to a level that can meet the current cyber threat.

4. SUPPLEMENT IN-HOUSE CAPABILITIES WITH THIRD-PARTY EXPERTISE

It can be difficult for government entities—particularly at the state and local level—to have sufficient in-house resources to implement all cybersecurity tactics, conduct all assessments, stay abreast of numerous legislative and regulatory requirements and engage in forensics, should a breach occur.

The 2016 Nationwide Cyber Security Review* found government bodies outsource little of their IT security operations to third parties; for example, 92 percent of local governments and 79 percent of state governments reported not outsourcing any cybersecurity operations. But third parties can:

• Help conduct capability, risk, vulnerability and impact assessments
• Scan networks for threats and implement corrective actions
• Develop cybersecurity strategy by applying deep knowledge of related legal, technical, communications and other subject areas
• Provide rigorous, ongoing training and awareness initiatives

Cybersecurity is a challenge for every organization. Local, state and federal government agencies are being targeted by a range of threat actors whose capabilities and persistence continue to grow. Taking action now to improve cyber risk management and implement best practices can help governments guard their networks and the data that passes through them.

“WITHOUT CYBERSECURITY TRAINING, 30 TO 60 PERCENT OF INDIVIDUALS FELL FOR A SOCIAL ENGINEERING ATTACK”

*The Nationwide Cyber Security Review is an offering of the Multi-State Information Sharing & Analysis Center® (MS-ISAC®). CIS® (Center for Internet Security) is the home of MS-ISAC.